

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

531 Smith Avenue, Apartment 2
Xenia, Ohio, 45385

Case No.

3:18mj507

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A-5

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

See Attachment B-5

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

See Attachment C-5

Offense Description

The application is based on these facts:
See Attached Affidavit

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Andrea R. Kinzig

Applicant's Signature

Andrea R. Kinzig, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 7-12-18

City and state: Dayton, Ohio

Sharon L. Ovington

Judge's signature

Sharon L. Ovington, U.S. Magistrate Judge

Printed name and title

FILED
RICHARD W. NAGEL
CLERK OF COURT
2018 JUL 12 PM 3:46
U.S. DISTRICT COURT
SOUTHERN DIST. OHIO
DAYTON

ATTACHMENT A-5

DESCRIPTION OF LOCATION TO BE SEARCHED

531 SMITH AVENUE, APARTMENT 2, XENIA, OHIO, 45385 ("SUBJECT PREMISES-2"), is contained in a two-story brick building with white shutters around the windows and white pillars around the front door. The street address numbers are black in color and affixed to a pillar next to the front door. Apartment 2 is located on the second story of the building. The SUBJECT PREMISES-2 is located on the east side of Smith Avenue between Weaver Street and Sutton Drive.

The search warrant will only be executed if location information for the cellular telephone bearing telephone number 937-516-6102 (as obtained pursuant to a search warrant authorized by the United States District Court for the Southern District of Ohio) identifies that the telephone is inside the SUBJECT PREMISES-2.



M40000200030002100 03/06/2012

ATTACHMENT B-5

LIST OF ITEMS TO BE SEIZED AND SEARCHED

Items evidencing violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1) (possession and attempted of child pornography); 18 U.S.C. §§ 2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography); and 18 U.S.C. §2251(a) and (e) (production of child pornography), including but not limited to the following:

1. The person of David Weaver, who is a white male, 38 years old, approximately five feet nine inches tall, weighing approximating 155 pounds, having brown hair and green eyes.
2. Cellular telephone bearing telephone number 937-516-6102 and International Mobile Subscriber Identity (IMSI) 310120068908119.
3. The personal belongings of David Weaver for Computer and Electronic Media:
 - a. Computer hardware, meaning any and all computer equipment, including any electronic devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical and compact disk storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone generating devices); any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks); cellular telephones and tablets; and digital cameras and recording devices.
 - b. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

- c. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
- d. Computer passwords and data security devices, meaning any devices, programs, or data -- whether themselves in the nature of hardware or software -- that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer-related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips, and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form.
- e. Any computer or electronic records, documents, and materials referencing or relating to the above-described offenses. Such records, documents, or materials, as well as their drafts or modifications, may have been created or stored in various formats, including, but not limited to, any hand-made form (such as writing or marking with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negative, video tapes, motion pictures, or photocopies); any mechanical form (such as photographic records, printing, or typing); any electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact disks); or any information on any electronic or magnetic storage device (such as floppy diskettes, hard disks, CD-ROMs, optical disks, printer buffers, sort cards, memory calculators, electronic dialers, or electronic notebooks), as well as printouts or readouts from any magnetic storage device.
- f. Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), of any computer or computer system. The form that such information might take includes, but is not limited to, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, CD-ROM disks, video cassettes, and other media capable of storing magnetic or optical coding.
- g. Any electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data used to conduct computer or Internet-based communications, or which contains material or data obtained through computer or Internet-based communications, including data in the form of electronic records, documents, and materials, including those used to facilitate interstate communications, including but not limited to telephone (including mobile telephone), tablets, and Internet Service Providers. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment, such as fixed disks, external hard disks, removable hard disk

cartridges, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, laser disks, or other memory storage devices.

Photographs of Search

4. During the course of the search, photographs of the SUBJECT PREMISES-2 may also be taken to record the condition thereof and/or the location of items seized from the residence.

ATTACHMENT C-5

<u>Code Section</u>	<u>Offense Description</u>
18 U.S.C. §2252(a)(4)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §2252A(a)(5)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §2252(a)(2)(B) & (b)(1)	Receipt and Distribution of Child Pornography
18 U.S.C. §2252A(a)(2) & (b)(1)	Receipt and Distribution of Child Pornography
18 U.S.C. §2251(a) and (e)	Production of Child Pornography

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a) and 2252A) and coercion and enticement (in violation of 18 U.S.C. §2422). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.
2. Along with other agents, officers, and investigators of the Broward County (Florida) Sheriff's Office, South Florida Internet Crimes Against Children (ICAC) Task Force, and FBI, I am currently involved in an investigation of child pornography and child exploitation offenses committed by **DAVID WEAVER**. This Affidavit is submitted in support of Applications under Rule 41 of the Federal Rules of Criminal Procedure for search warrants for the following:
 - a. The residential property located at 2212 Neff Road, Dayton, Ohio, 45414 (hereinafter referred to as the "**SUBJECT PREMISES-1**" and more fully described in Attachment A-1 hereto);
 - b. The person of **DAVID WEAVER** (hereinafter referred to as "**WEAVER**" and more fully described in Attachment A-2 hereto);
 - c. 2015 Dodge Dart bearing Ohio license plate GZA7050, orange in color (hereinafter referred to as "**SUBJECT VEHICLE**" and more fully described in Attachment A-3 hereto);
 - d. Cellular telephone bearing telephone number **937-516-6102** and International Mobile Subscriber Identity (IMSI) 310120068908119 (hereinafter referred to as "**SUBJECT DEVICE**" and more fully described in Attachment A-4 hereto); and
 - e. The residential property located at 531 Smith Avenue, Apartment 2, Xenia, Ohio, 45385 (hereinafter referred to as "**SUBJECT PREMISES-2**" and more fully described in Attachment A-5 hereto).
3. This Affidavit is submitted in support of Applications for search warrants for the **SUBJECT PREMISES-1**, **SUBJECT PREMISES-2**, the person of **WEAVER**, the **SUBJECT VEHICLE**, the **SUBJECT DEVICE**, and the Computer and Electronic

Media (as defined in Attachments B-1 through B-5) located at the **SUBJECT PREMISES-1, SUBJECT PREMISES-2**, on the person of **WEAVER**, and in the **SUBJECT VEHICLE**. The purpose of the Applications is to seize evidence of violations of the following:

- a. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1), which make it a crime to possess child pornography;
 - b. 18 U.S.C. §§ 2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1), which make it a crime to distribute and receive child pornography through interstate commerce; and
 - c. 18 U.S.C. §§ 2251(a) and (e), which make it a crime to produce child pornography.
4. The items to be searched for and seized are described more particularly in Attachments B-1 through B-5 hereto and are incorporated by reference.
 5. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents, officers, and investigators involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.
 6. This Affidavit does not contain every fact known to the investigation, but only those deemed necessary to demonstrate sufficient probable cause to support the searches of the **SUBJECT PREMISES-1, SUBJECT PREMISES-2**, the person of **WEAVER**, the **SUBJECT VEHICLE**, the **SUBJECT DEVICE**, and the Computer and Electronic Media (as defined in Attachments B-1 through B-5) located at the **SUBJECT PREMISES-1, SUBJECT PREMISES-2**, on the person of **WEAVER**, and in the **SUBJECT VEHICLE**.
 7. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence of a crime, contraband, fruits of crime, or other items illegally possessed, property designed for use, intended for use, or used in committing a crime of violations of federal law, including 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1), 2252A(a)(5)(B) and (b)(1), 2252(a)(2)(B) and (b)(1), 2252A(a)(2) and (b)(1), and 2251(a) and (e) are present at the **SUBJECT PREMISES-1, SUBJECT PREMISES-2**, on the person of **WEAVER**, in the **SUBJECT VEHICLE**, on the **SUBJECT DEVICE**, and on the Computer and Electronic Media (as defined in Attachments B-1 through B-5) located at the **SUBJECT PREMISES-1, SUBJECT PREMISES-2**, on the person of **WEAVER**, and in the **SUBJECT VEHICLE**.

PERTINENT FEDERAL CRIMINAL STATUTES

8. 18 U.S.C. § 2252(a)(4)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or attempt to do so.
9. 18 U.S.C. § 2252A(a)(5)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or attempt to do so.
10. 18 U.S.C. § 2252(a)(2)(B) and (b)(1) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or attempt to do so.
11. 18 U.S.C. § 2252A(a)(2) and (b)(1) states that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or attempt to do so.
12. 18 U.S.C. §§ 2251(a) and (e) states that it is a violation for any person to knowingly employ, use, persuade, induce, entice, or coerce any minor to engage in, or to have a minor assist any other person to engage in, or to transport any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live

visual depiction of such conduct, when he knew or had reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or attempts or conspires to do so.

BACKGROUND INFORMATION

Definitions

13. The following definitions apply to this Affidavit and Attachments B-1 through B-5 to this Affidavit:
- a. **“Child Pornography”** includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).
 - b. **“Visual depictions”** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).
 - c. **“Minor”** means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).
 - d. **“Sexually explicit conduct”** means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. § 2256(2)).
 - e. **“Internet Service Providers”** or **“ISPs”** are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data,

called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

- f. An “**Internet Protocol address**”, also referred to as an “**IP address**”, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as “octets,” ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).
- g. “**Hyperlink**” (often referred to simply as a “link”) refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. “resource”) to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.
- h. “**Website**” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
- i. “**Uniform Resource Locator**” or “**Universal Resource Locator**” or “**URL**” is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.
- j. A “**Smartphone**” is a mobile cellular telephone that performs many of the functions of a computer, typically having a touchscreen interface, Internet access,

and an operating system capable of running downloaded applications.

- k. **Wi-Fi** is a technology that allows electronic devices to connect to a wireless LAN network. Devices that use Wi-Fi technology include personal computers, video game consoles, smartphones, digital cameras, tablets, and modern computers.
- l. A “**digital camera**” is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- m. “**SMS**” or “**Short Message Service**” is a text messaging service component of most telephone, Internet, and mobile-device systems. It uses standardized communication protocols to enable mobile devices to exchange short text messages. An intermediary service can facilitate a text-to-voice conversion to be sent to landlines.
- n. “**MMS**” or “**Multimedia Messaging Service**” is a standard way to send messages that include multimedia content (including images and videos) to and from a mobile phone over a cellular network. The MMS standard extends the core SMS capability, allowing the exchange of text messages greater than 160 characters in length.
- o. The terms “**records**,” “**documents**,” and “**materials**,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

Background on Computers and Child Pornography

- 14. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically

serve four functions in connection with child pornography: production, communication, distribution, and storage.

15. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.
16. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.
17. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person.
18. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.
19. Individuals also use online resources to retrieve and store child pornography, including

services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

20. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

Collectors of Child Pornography

21. Based upon my knowledge, training, and experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter "collectors"):
 - a. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.\
 - b. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.
 - c. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.
 - d. Collectors almost always possess and maintain their "hard copies" of child

pornographic images and reference materials (e.g., mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the collector's residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods of time, even for years. Collectors often discard child pornography images only while "culling" their collections to improve their overall quality.

- e. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.
- f. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
- g. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during several recent nationwide law enforcement initiatives.

Google Email and Photos

- 22. Google LLC is a multi-national corporation with its headquarters located in Mountain View, California. The company specializes in Internet-related products and services, including an Internet search engine (www.google.com), productivity tools such as email service (gmail), and enterprise products such as Google Search Appliance.
- 23. Google Photos is a photograph and video sharing and storage service provided by Google LLC, located at photos.google.com. It allows users to back-up their photographs and videos so they can be accessed on any telephone, tablet, or computer. It also allows users to pool their photographs and videos together with others into shared albums. Photographs and videos can be organized and searched by places and things in them.

NCMEC and CyberTipline Reports

- 24. The National Center for Missing and Exploited Children (commonly known as "NCMEC") was founded in 1984 to serve as a clearinghouse on issues related to missing and sexually exploited children. It is currently authorized by Congress to perform 19 programs and services to assist law enforcement, families, and professions find missing children, reduce child sexual exploitation, and prevent child victimization.

25. As part of its functions, NCMEC administers the CyberTipline. The CyberTipline receives leads and tips from the public and Electronic Service Providers regarding suspected crimes of sexual exploitation committed against children. Electronic Service Providers are required by law to report apparent child pornography to law enforcement via the CyberTipline. Analysts review these tips and refer them to the appropriate federal, state, and local law enforcement authorities.

FACTS SUPPORTING PROBABLE CAUSE

26. Beginning in or around July 2017, the Broward County Sheriff's Office and South Florida ICAC have investigated Russell Schroeder (hereinafter referred to as "Schroeder") for child pornography offenses. On or around March 14, 2018, a search warrant authorized by the Broward County (Florida) Circuit Court was executed at Schroeder's residence in Oakland Park, Florida. Various electronic media were seized pursuant to the search warrant, including an Apple iPhone belonging to Schroeder. Schroeder was interviewed by law enforcement officers before and during the execution of the search warrant, and he admitted that he was involved in viewing child pornography.
27. Schroeder's iPhone was subsequently examined pursuant to the search warrant. The examination recovered more than twenty-two thousand image and video files depicting child pornography. The examination also determined that Schroeder obtained and traded child pornography files via a variety of means.
28. Law enforcement officers identified that a contact was saved in Schroeder's iPhone under the name of "David". Listed in the contact information for "David" was the telephone number 937-516-6648 (hereinafter referred to as the "TARGET TELEPHONE") and the email address ddweaver937@gmail.com.
29. Approximately 10 MMS messages were recovered from Schroeder's iPhone that were sent from Schroeder to "David" via the TARGET TELEPHONE during the approximate time period of August 22, 2017 through January 3, 2018. These MMS messages contained approximately seventeen image files and three video files. I have reviewed these files, and based on my training and experience, I believe that at least approximately thirteen of the images and at least approximately one of the videos depict child pornography (as defined by 18 U.S.C. § 2256(8)). By way of example, two of the files are described as follows:
- a. IMG_4960.jpg: The file is an image that depicts what appears to be an infant or toddler-aged male child lying on his back. The penis of what appears to be an adult white male (whose face is not captured in the image) is in the baby's mouth.
 - b. IMG_2152.jpg: The file is an image that depicts what appears to be a nude adult white male (whose face is not captured in the image) lying on his back. What appears to be a nude pre-pubescent male child is squatting over the adult male's groin area. The penis of the adult male is inserted into the child's anus.

30. Approximately 19 SMS messages were recovered from Schroeder's iPhone that were exchanged between Schroeder and "David" via the TARGET TELEPHONE during the approximate time period of August 17, 2017 through January 9, 2018. Based on the context of these messages and my training and experience, it appears that Schroeder and "David" were discussing child pornography files that "David" had sent to Schroeder. It was noted that "David" and Schroeder both indicated that these files depicted "David" engaging in sexual activities with "David's" son. However, no MMS messages were recovered from the iPhone containing image or video files that were sent from "David" to Schroeder. As such, it appears that Schroeder deleted these files from his Inbox (possibly after saving the files to another secure or permanent location) or that the files were sent by "David" to Schroeder via another platform (such as email, another messenger application, social media, etc.). The messages also indicate that Schroeder and "David" communicated with each other via other platforms, including Telegram (an encrypted messenger application) and Tumblr (a social media application). Below are excerpts of these SMS messages:

August 17, 2017:

David: He is one of me fucking my son a month ago

Schroeder: Damn! Fucking nice. Thank you

August 20, 2017:

Schroeder: Hey buddy. The last video was hot. Any others you want to send me of you fucking young boys I'll take. Makes my dick so fucking hard.

Schroeder: What's your Telegram screen name again? Catch ya buddy.

David: Use my telephone number 937 516 6648

Schroeder: Ok. But aren't you on telegram too?

David: Thats how u find me on telegram

David: I am at work

Schroeder: I know. Sorry. Enjoy in the john. I'm off to sleep now. Nite.

David: Thanks

August 21, 2017:

Schroeder: Actually I found you on Tumbler.

Schroeder: Is this going to your phone?

David: Yes

.....

August 26, 2018:

Schroeder: Hey bud! Any good stuff for me? Want to see you fucking that son of yours when he was really young. Woof!!!

.....

January 9, 2018:

Schroeder: Hey buddy! Any good stuff you can send me? Love seeing you fuck your son

31. A detective of the Broward County Sheriff's Office served a subpoena to Google LLC requesting subscriber information for the ddweaver937@gmail.com account and logs of IP addresses utilized to access the account. Records received in response to the subpoena provided the following information:
 - a. The account was subscribed to in the name of "David Weaver". The TARGET TELEPHONE was listed as the account user's telephone number.
 - b. The account was opened on or around January 1, 2017, and was closed on or around April 20, 2018.
 - c. A number of IP addresses associated with Sprint Corporation's network were utilized to access the account. Based on my training and experience, I know that this account activity is consistent with someone using the data plan from his/her cellular telephone to access the Internet and log into his/her email account.
32. Based on the records obtained from Google LLC, the detective from the Broward County Sheriff's Office queried the name "David Weaver" in law enforcement databases. Records were located for **WEAVER** which indicated that he previously resided in Florida but currently resided in Dayton, Ohio. The detective thereafter contacted me and forwarded me the information regarding her investigation of **WEAVER**.
33. As part of the investigation, I have learned that Google LLC has filed approximately 17 CyberTipline reports regarding suspected child pornography files located in Google accounts associated with the TARGET TELEPHONE. In these reports, Google LLC reported that the company had located a total of approximately 43 suspected child pornography files in five separate Google accounts. Below is a summary of these reports:
 - a. In or around May 2018, Google LLC filed a CyberTipline report regarding the Google account ddweaver1984@gmail.com. The report identified that the Google account was subscribed to in the name of "David Weaver", and the TARGET TELEPHONE was listed as the account user's telephone number. The report further identified that Google LLC discovered approximately three suspected child pornography files in the Google Photos account associated with this email address. According to the report, these files were uploaded to the Google Photos account on or around February 23, 2018.
 - b. During the approximate time period of October 2017 through May 2018, Google LLC filed approximately nine CyberTipline reports regarding the Google account ddweaver937@gmail.com. The report identified that the Google account was subscribed to in the name of "David Weaver", and the TARGET TELEPHONE

was listed as the account user's telephone number. The report further identified that Google LLC discovered a total of approximately 35 unique suspected child pornography files in the Google Photos account associated with this email address. According to the report, these files were uploaded to the Google Photos account on or around September 20, 2017 and October 10, 2017.

- c. In or around February 2017, Google LLC filed a CyberTipline report regarding the Google account ddweaver1998@gmail.com. The report identified that the Google account was subscribed to in the name of "David Weaver", and the TARGET TELEPHONE was listed as the account user's telephone number. The report further identified that Google LLC discovered approximately one suspected child pornography file in the Google account associated with this email address. The report did not specify if the file was discovered in the Google Photos account or another part of the account. According to the report, the file was uploaded to the Google account on or around February 2, 2017.
- d. In or around November 2016, Google LLC filed a CyberTipline report regarding the Google account downtoearthguy@gmail.com. The report identified that the TARGET TELEPHONE was the account user's telephone number, but no subscriber name was listed for the account. The report further identified that Google LLC discovered approximately three suspected child pornography files in the Google account associated with this email address (one of which was the same as one of the files in the ddweaver937@gmail.com account). The report identified that the suspected child pornography files were attached to an email message(s). According to the report, the files were uploaded to the Google account on or around November 9, 2016.
- e. In or around September 2016, Google LLC filed a CyberTipline report regarding the Google account ddweaver1229@gmail.com. The report identified that the TARGET TELEPHONE was the account user's telephone number, but no subscriber name was listed for the account. The report further identified that Google LLC discovered approximately one suspected child pornography file in the Google account associated with this email address (which was the same as one of the files in the downtoearthguy@gmail.com account). The report identified that the suspected child pornography file was attached to an email message. According to the report, the file was uploaded to the Google account on or around September 13, 2016.
- f. In the reports detailed above, Google LLC provided the IP addresses that were utilized by the account user(s) to upload the suspected child pornography files. Review of the IP addresses identified that most of them were serviced by Sprint Corporation. As previously noted, I know that this account activity is consistent with someone using a data plan from his/her cellular telephone to access the Internet.

34. As part of filing the CyberTipline reports, Google LLC provided to NCMEC the

suspected child pornography files that were located in the five Google accounts listed above. Based on the information provided by Google LLC in its CyberTipline reports, employees of Google LLC did not view approximately 11 of the files.

35. As part of the investigation, I have obtained from NCMEC the files submitted by Google LLC as part of its CyberTipline reports. The files are contained on two disks – one that contains the files that have been viewed by employees of Google LLC and one that contains the approximately 11 files that have not been viewed by employees of Google LLC. As such, it appears that Google LLC identified these 11 files using a tool that detects child pornography files based on known hash values, photo DNA, or another means. Pursuant to *U.S. v. Keith*, 2013 WL 5918524 (D. Mass. 2013), at this time I have only viewed the disk containing the files that have been viewed by employees of Google LLC. Based on my review of the files and my training and experience, I believe that approximately 32 of the files depict child pornography (as defined by 18 U.S.C. § 2256(8)). By way of example, five of the files are described as follows:
 - a. 7eff0132-53a5-4077-b4fe-0a872ee02368.png: The file is an image that depicts what appears to be the anus of a pre-pubescent white male child whose legs are spread apart. The file was located in the downtoearthguy30@gmail.com Google account.
 - b. IMG_8716.jpg: The file is an image that depicts what appears to be two nude black male children, one of whom is adolescent and one of whom is pre-pubescent. The two male children are standing in a bathroom, and their penises are exposed to the camera. The file was located in ddweaver1984@gmail.com Google account.
 - c. b7e70294ccf5a735bf21d557d153ee.jpg: The file is an image that depicts what appears to be an adolescent white male child who is wearing pants but no shirt and who is standing in front of a mirror. The child's erect penis is pulled over his pants. The file was located in the ddweaver1998@gmail.com Google account.
 - d. imgsrc.ru_50346683sJt.jpg: The file is an image that depicts what appears to be a nude pre-pubescent Asian male child who is lying on his back and a nude pre-pubescent white female child who is lying on her side. The penis of the male child is in the female child's mouth. The file was located in the ddweaver937@gmail.com Google account.
 - e. JOEL-M-S2020088a .jpg: The file is an image that depicts what appears to be a nude pre-pubescent Asian male child who is lying on his back with his legs straddled above his head and a nude adult white male (whose face is not captured in the image). It appears that the adult male's penis is in the child's anus and that the child is screaming. The file was located in the ddweaver937@gmail.com Google account.
36. It was noted that the one file that Google LLC reported in its CyberTipline report for the

ddweaver1229@gmail.com account is one of the files that was not been viewed by employees of Google LLC. Based on the presence of verified child pornography files in the other four email accounts associated with the TARGET TELEPHONE, it is reasonable to believe that the ddweaver1229@gmail.com Google account also contains child pornography and/or child abuse material.

37. Review of records from the Ohio Bureau of Motor Vehicles identified that **WEAVER** currently utilizes the **SUBJECT PREMISES-1** on his current Ohio driver's license. Records from the Ohio Bureau of Motor Vehicles also determined that one motor vehicle is currently jointly registered to **WEAVER** and another adult female at the **SUBJECT PREMISES-1** – that being the **SUBJECT VEHICLE**. Based on review of public records, I have determined that this adult female is deceased. On or around June 30, 2018, I observed the **SUBJECT VEHICLE** parked in front of the **SUBJECT PREMISES-1**.
38. As part of the investigation, I have obtained information and reports from other law enforcement agencies regarding prior contacts with **WEAVER**. These records have provided the following information:
 - a. On or around July 1, 2017, **WEAVER** was involved in a traffic accident in Riverside, Ohio while driving the **SUBJECT VEHICLE**. As part of completing the accident report, the responding officers collected information from **WEAVER**. **WEAVER** told the officer that he resided at the **SUBJECT PREMISES-1** and that his telephone number was the TARGET TELEPHONE.
 - b. On or around July 13, 2017, **WEAVER** reported to the Dayton (Ohio) Police Department that an unknown male assaulted him with a stun gun and stole his vehicle and cellular telephone. **WEAVER** identified that he was driving a rental vehicle because his vehicle was currently being repaired. **WEAVER** identified that the telephone that was stolen from him was an LG Tribute cellular telephone bearing telephone number 937-516-6648 (the TARGET TELEPHONE). **WEAVER** told one of the responding officers that he resided at the **SUBJECT PREMISES-1**.
 - c. On or around August 29, 2017, **WEAVER** was cited for speeding in Huber Heights, Ohio while driving the **SUBJECT VEHICLE**. During the traffic stop, **WEAVER** told the officer that he resided at the **SUBJECT PREMISES-1**.
39. Sprint Corporation was identified as the service provider for the TARGET TELEPHONE. On or around June 28, 2018, an FBI investigator served Sprint Corporation with an administrative subpoena requesting subscriber information for this telephone number. Records received in response to the subpoena identified that the telephone number was subscribed to **WEAVER** at the **SUBJECT PREMISES-1**. The records identified that **WEAVER** obtained new cellular telephone devices while keeping the same telephone number (937-516-6648) on or around July 16, 2017 and again on July 22, 2017 (shortly after he reported to the Dayton Police Department that his telephone

was stolen, as detailed above). The records also identified that **WEAVER** obtained a new telephone number on or around May 25, 2018, while keeping the same device. Sprint Corporation's records identified that **WEAVER**'s telephone account was assigned the Subscriber ID of 70377065121 and the Billing Account Number of 434836173.

40. On or around July 2, 2018, an FBI investigator served Sprint Corporation with an additional subpoena requesting subscriber information regarding the new cellular telephone number assigned to **WEAVER**'s subscriber and billing account. Results of the subpoena identified that the new telephone number was **937-516-6102** (the number assigned to the **SUBJECT DEVICE**), and that the IMSI for the current device was 310120068908119.
41. On or around July 9, 2018, a search warrant was authorized by the United States District Court for the Southern District of Ohio for the cellular telephone assigned call number **937-516-6102** (the number assigned to the **SUBJECT DEVICE**). This search warrant authorized the release of location information (i.e., cell site, cell sector, and GPS information) for the **SUBJECT DEVICE** by Sprint Corporation for a period of 30 days. Pursuant to the search warrant, Sprint Corporation began providing the requested location information for the **SUBJECT DEVICE** to the FBI during the early morning hours of July 10, 2018. Sprint Corporation provided the approximate location (expressed in the latitude, longitude, and a measurement of uncertainty) of the telephone every approximately 15 minutes. The location information provided by Sprint Corporation during the time period of the early morning hours of July 9, 2018 through the afternoon hours of July 12, 2018 provided the following information:
 - a. From approximately the early morning hours through the late evening hours of July 10, 2018, the **SUBJECT DEVICE** was consistently in the area of the **SUBJECT PREMISES-1**.
 - b. From approximately the late evening hours of July 10, 2018 through the present, the **SUBJECT DEVICE** was primarily in the area of the **SUBJECT PREMISES-2** (although it left for a brief period of time on at least one occasions, thereafter returning to the residence).
 - c. The **SUBJECT DEVICE** was located in the Southern District of Ohio at all times.
42. On or around July 12, 2018, an officer of the Xenia (Ohio) Police Department contacted the occupants of the **SUBJECT PREMISES-2** under a ruse. An adult male who will be referred to for purposes of this Affidavit as "Adult Male A" opened the door and allowed the officer to enter the residence. The officer thereafter encountered **WEAVER** sitting on a chair in the Living Room. Adult Male A identified that he lived at the residence and that **WEAVER** was visiting him. Based on this and other information noted in the Affidavit, there is probable cause to believe that **WEAVER** resides at the **SUBJECT PREMISES-1** but is currently staying with Adult Male A at the **SUBJECT PREMISES-2**.

43. Based on all of the information detailed above, I believe that **WEAVER** is the user of the TARGET TELEPHONE, the **SUBJECT DEVICE**, and the email addresses ddweaver1984@gmail.com, ddweaver937@gmail.com, ddwewaver1998@gmail.com, downtoearthguy@gmail.com, and ddweaver1229@gmail.com. I also believe that he has utilized the TARGET TELEPHONE, the **SUBJECT DEVICE**, and/or the noted email accounts to possess, receive, distribute, and produce child pornography.
44. Based on my training and experience, I know that it is not uncommon for individuals involved in child pornography offenses to utilize multiple computer devices in furtherance of their child pornography and child exploitation activities. Individuals sometimes save their files to multiple devices to allow easy access to the files and/or to back-up the devices in case of a computer failure.
45. Again based on my training and experience, I know that collectors of child pornography often use external devices (such as thumb drives, external hard drives, CD's/DVD's, SD cards, SIM cards, etc.) to store child pornography. The accumulation of child pornography files may fill up the space on the hard drives of computers, and external devices are needed to store and maintain files. These devices also serve as a mechanism for transferring files from one computer to another. In my experience, individuals maintain such external devices in their residences. Given their portable size, individuals sometimes maintain the devices on their persons and/or take the devices with them when they travel by vehicle.
46. Based on my training and experience, I know that individuals are increasingly utilizing laptop computers and other smaller devices such as cellular telephones, iPads, and tablets to do their computing. These devices are typically maintained in the owners' residences. Due to their portable nature, individuals also sometimes maintain the devices on their persons and/or take the devices with them when they travel by vehicle.
47. Based on my training and experience, I know that collectors of child pornography often maintain their collections for long periods of time. In addition, computer evidence typically persists for long periods of time, and computer data can often be recovered from deleted space (as further detailed above).
48. Based on my training and experience, individuals involved in child exploitation schemes often utilize social media accounts, email addresses, messenger applications, and dating websites as a means to locate and recruit victims. They then use the chat functions on these websites, as well as email accounts and other messenger applications, to communicate with their victims. Such communications provide a means of anonymity to protect the subjects' identities and to conceal the communications from the victims' parents.
49. Also based on my training and experience, I know that individuals involved in child exploitation offenses utilize a variety of threats and manipulation techniques to compel their victims to engage or continue engaging in the illicit sexual activities (including the

production of child pornography). These threats and manipulations are intended to control the victims and their activities, prevent them from stopping the activities, and prevent them from contacting law enforcement officers. It is common for such offenders to threaten that if the victims end the illicit sexual activities, the offenders will harm the victims and their family members and / or bring notoriety and shame to the victims by exposing the victims' involvement in the sexually explicit conduct.

50. In my experience, individuals involved in child exploitation schemes often communicate with others involved in similar offenses via e-mail, social media, and other online chatrooms. I have seen examples of cases where such individuals have communicated with other child predators about their sexual fantasies and prior sexual activities with juveniles. I have also seen cases where such individuals have communicated with others about their remorse and regret for their activities. Both types of communications provide material evidence in child exploitation cases in that they provide admissions of guilt.
51. In my experience, individuals often attempt to obtain child pornography from a variety of sources, including from those with whom they communicate via email, social media sites, Internet chat programs, and on Internet bulletin boards; Internet P2P file sharing programs; Internet websites; and other sources. Evidence of multiple aliases, accounts, and sources of child pornography can often be found in the subjects' email communications. Evidence of the multiple aliases, accounts, and sources of child pornography are often found on the computer devices located at the offenders' residences, in their vehicles, and on their persons.
52. I know, in my experience, that individuals involved in child exploitation offenses sometimes print the pictures in hard copy format. Such individuals do so both for easier access / viewing of the files and to back-up the files in the event that one computer device becomes damaged and broken. Similarly, these individuals often save contact information (i.e., email addresses and account names) for those with whom they communicate about child exploitation offenses in multiple locations.
53. In addition, individuals often maintain lists of their electronic accounts (including associated user names and passwords) and their aliases in handwritten format. These papers are sometimes maintained in close proximity to their computers for easy access. In other cases, the papers may be hidden or maintained in secure locations to avoid detection by others.
54. In my experience, I know that many cellular telephones, iPads, and tablets store information related to IP addresses and Wi-Fi accounts that the telephone accessed and GPS data. This information helps in identifying the subjects' whereabouts during the criminal activities and the travels they took to get to these locations.

CONDITIONAL AUTHORITY FOR SUBJECT PREMISES-2

55. As detailed above, the location information obtained from the **SUBJECT DEVICE** and information obtained by the Xenia Police Department has identified that **WEAVER** and

the **SUBJECT DEVICE** have been at the **SUBJECT PREMISES-2** since the evening hours of July 10, 2018. As detailed above, I know that individuals often take laptops, computers, smaller electronic devices (such as cellular telephones, iPads, and tablets), and external devices (such as thumb drives, external hard drives, CD's/DVD's, SD cards, SIM cards, etc.) with them when they travel, particularly if they plan to be gone for multiple days.

56. If the location information from the **SUBJECT DEVICE** indicates that it is located inside the **SUBJECT PREMISES-2** at the time that the warrants for **WEAVER** and the **SUBJECT DEVICE** will be executed, authority is requested pursuant to the proposed search warrant for the **SUBJECT PREMISES-2** to enter the residence and search for the items listed in Attachment B-5. If the location information identifies that the **SUBJECT DEVICE** is no longer located at the **SUBJECT PREMISES-2**, the search warrant for the **SUBJECT PREMISES-2** will not be executed.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

57. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:
 - a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.
 - b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.
58. In order to fully retrieve data from a computer system, the analyst needs all magnetic

storage devices as well as the central processing unit (“CPU”). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

59. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

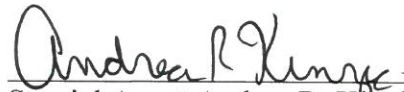
SEARCH METHODOLOGY TO BE EMPLOYED REGARDING ELECTRONIC DATA


60. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):
- a. On-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software;
 - b. On-site forensic imaging of any computers that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for examination; such imaging may require several hours to complete and require law enforcement agents to secure the search scene until that imaging can be completed;
 - c. Examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
 - d. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
 - e. Surveying various file directories and the individual files they contain;
 - f. Opening files in order to determine their contents;
 - g. Scanning storage areas;

- h. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachments B-1 and B-2; and
- i. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachments B-1 through B-5.

CONCLUSION

- 61. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence of a crime, contraband, fruits of crime, or other items illegally possessed, property designed for use, intended for use, or used in committing a crime of violations of federal law, may be located at the **SUBJECT PREMISES-1, SUBJECT PREMISES-2**, on the person of **WEAVER**, in the **SUBJECT VEHICLE**, on the **SUBJECT DEVICE**, and on the Computer and Electronic Media (as defined in Attachments B-1 and B-5) located at the **SUBJECT PREMISES-1, SUBJECT PREMISES-2**, on the person of **WEAVER**, and in the **SUBJECT VEHICLE**: 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1), 2252A(a)(5)(B) and (b)(1), 2252(a)(2)(B) and (b)(1), 2252A(a)(2) and (b)(1), and 2251(a) and (e).
- 62. I, therefore, respectfully request that the attached warrants be issued authorizing the search and seizure of the items listed in Attachments B-1 through B-5.


Special Agent Andrea R. Kinzig
Federal Bureau of Investigation

SUBSCRIBED and SWORN
Before me this 12th of July 2018

SHARON L. OVINGTON
UNITED STATES MAGISTRATE JUDGE